

REMARKS

In the non-final Office Action, the Examiner objects to claim 2 because of an alleged informality; rejects claims 1, 2, 9-14, 16, and 17 under 35 U.S.C. § 102(e) as being allegedly anticipated by COOPER et al. (U.S. Patent Application Publication No. 2004/0039942); rejects claims 3-6, 15, 18, and 22 under 35 U.S.C. § 103(a) as being allegedly unpatentable over COOPER et al. in view of HADDOCK et al. (U.S. Patent No. 6,678,248); rejects claims 7 and 8 under 35 U.S.C. § 103(a) as being allegedly unpatentable over COOPER et al. in view of WESTERINEN (U.S. Patent No. 6,119,185); and rejects claims 19, 21, 23, and 24 under 35 U.S.C. § 103(a) as being allegedly unpatentable over COOPER et al. in view of PIESCO (U.S. Patent Application Publication No. 2003/0212908). Applicant respectfully traverses the rejections under 35 U.S.C. §§ 102 and 103.

By way of this Amendment, claim 2 has been amended to improve form. Claims 1-12, 15-19, and 21-24 remain pending in the present application. Reconsideration and timely allowance of all claims in view of the preceding amendments and the following remarks are respectfully requested.

Claim Objections

Claim 2 stands objected to because of minor informalities. More specifically, paragraph 2 of the Office Action indicates that the recitation of “the at least one policy points” at lines 2 and 3 of claim 2 lacks a sufficient antecedent basis. Claim 2 has been amended to correct this alleged deficiency. Reconsideration and withdrawal of the objection to claim 2 are respectfully requested.

Rejection Under 35 U.S.C. 102(e) based on COOPER et al.

Claims 1, 2, 9-12, 16, and 17 stand rejected under 35 U.S.C. § 102(e) as being anticipated by COOPER et al. Applicant respectfully traverses this rejection.

As an initial matter, Applicant notes that the Examiner continues to reject claims 13 and 14 in the present rejection. Claims 13 and 14 were canceled without prejudice or disclaimer in the prior Amendment dated March 30, 2007. Withdrawal of the rejection of these claims is respectfully requested.

A proper rejection under 35 U.S.C. §102 requires that a single reference teach every aspect of the claimed invention either expressly or impliedly. Any feature not directly taught must be inherently present. In other words, the identical invention must be shown in as complete as contained in the claim. See M.P.E.P §2131. COOPER et al. does not disclose or suggest the combination of features recited in claims 1-2, 9-14, 16-17, 19-21 and 23-26.

For example, independent claim 1 is directed to a method of analyzing policy rules defined for a subscriber and determining packet treatment. The method includes retrieving definitions pertaining to policy rules for a subscriber; determining at least one policy point in a network for the subscriber based on the retrieved definitions; determining the packet treatment at each of the at least one policy point; and outputting information corresponding to the packet treatment for each of the at least one policy point. COOPER et al. does not disclose or suggest the combination of features recited in claim 1.

More specifically, COOPER et al. does not disclose or suggest determining at least one policy point in a network for a subscriber based on the retrieved definitions, as

recited in claim 1. In rejecting claim 1, the Examiner cited page 8, paragraphs [0170]-[0171] and page 9, paragraph [0207] of COOPER et al. for allegedly disclosing this feature (Office Action – pg. 3). Applicant respectfully disagrees with the Examiner's interpretation of COOPER et al.

At page 8, paragraph [0170]-[0171], COOPER et al. discloses:

Identify the Policy Domains

FIG. 11 shows a high-level view of an example network. An Intranet 1101 is connected to a DMZ 1102 through a firewall 1103. The DMZ 1102, in turn, connects through a router 1104 to the Internet 1105 and through a second router 1106 to an external corporate network 1107. In this example, an end user is only expected to be able to monitor traffic in the Intranet and DMZ, so these two entities are declared to be policy domains. Rules in the policy only apply to allowed traffic in the DMZ and Internet. The corporate network and Internet are viewed only as communities of hosts visible from within the policy domains.

This section of COOPER et al. discloses that “policy domains” include networks on which a user may be expected to be able to monitor traffic. In the case of Fig. 11 of COOPER et al., these networks include Intranet 1101 and DMZ 1102. This section of COOPER et al. does not disclose or suggest determining at least one policy point in a network for a subscriber based on the retrieved definitions, as recited in claim 1. The Examiner appears to be asserting that a policy domain as described in COOPER et al. is analogous to the at least one policy point of claim 1. Applicant respectfully refutes this interpretation of COOPER et al. Clearly, based on the portion of COOPER et al. recited above (and relied on by the Examiner), the term policy domain refers to networks that may have traffic rules applied to it, where the network may be a part of a larger network. Clearly this is not analogous to a policy point in a network, as recited in claim 1 and supported in the present specification.

Even assuming *arguendo* that the policy domain of COOPER et al. correlates to a policy point (a point that Applicant strenuously does not concede), COOPER et al. still does not disclose or suggest selecting the policy domain for a subscriber based on the retrieved definitions pertaining to policy rules for the subscriber, as required by claim 1.

At page 9, paragraph [0207], COOPER et al. discloses:

The Monitoring Point is a specification of where the Input dump file was collected. This name is derived from policy domain names that are specified in the policy wizard. For example, if a packet dump was collected in a policy domain named "Intranet" then the Monitoring Point name INTRANET_MONITOR should be used.

This section of COOPER et al. discloses that the point at which the input packet dump file was collected is named based on the policy domain in which the policy is being applied. This section of COOPER et al. does not disclose determining at least one policy point in a network for the subscriber based on the retrieved definitions, as required by claim 1. Rather, this section of COOPER et al. merely discloses assigning a name to the dump location from which packet data is collected, with the name being selected based on the policy domain being affected. Thus, the specification of the monitoring point is based on a user input of this information. Clearly, the collection point of COOPER et al. is not identified within the network for the subscriber based on the retrieved definitions, as required by claim 1.

For at least these reasons, claim 1 is not anticipated by COOPER et al.

Reconsideration and withdrawal of the rejection of claim 1 are respectfully requested.

Claims 2 and 9 depend from claim 1 and are therefore not anticipated by COOPER et al. for at least the reasons set forth above with respect to claim 1. Moreover, these claims are not anticipated by COOPER et al. for reasons of their own.

For example, COOPER et al. does not disclose or suggest consolidating the determined packet treatment for each of the at least one policy points, as required by claim 2. In rejecting claim 2, the Examiner indicates that page 22, paragraph [0362] of COOPER et al. allegedly discloses this feature (Office Action – pg. 3). Applicant respectfully disagrees.

At page 22, paragraph [0362]-[0363], COOPER et al. discloses:

It should be appreciated that using the invention as a supplemental process in performing network assessments results in at least the following benefits:

Rather than providing an inference of possible network behavior that is based on what hosts are configured to do, the network behavior is directly analyzed based on direct observation of the data traffic;

This section of COOPER et al. discloses analyzing network behavior by directly observing data traffic. This section of COOPER et al. does not disclose or even remotely suggest consolidating the determined packet treatment for each of the at least one policy points, as required by claim 2. In fact, this section of COOPER et al. does not disclose or discuss policy points or determining packet treatment whatsoever, let alone consolidating packet treatment determined at each policy point, as required by claim 2. Rather, this section of COOPER et al. discloses simply monitoring traffic on a network.

For at least this additional reason, claim 2 is not anticipated by COOPER et al. Reconsideration and allowance of claim 2 are respectfully requested.

COOPER et al. likewise fails to disclose or suggest determining at least one injection point based on the at least one policy point; using at least one policy agent to inject packets at the at least one injection point; or collecting statistics from some of the at least one policy agent, as required by claim 9. In rejecting claim 9, the Examiner indicated that page 9, paragraphs [0190] – [0207], page 14, paragraphs [0289] and

[0292], and page 4, TABLE A of COOPER et al. allegedly disclose these features (Office Action – pp. 3-4). Applicant respectfully disagrees with the Examiner's interpretation of COOPER et al.

Page 9, paragraphs [0190] to [0207] of COOPER et al. discloses that packet gathering component 128 collects packet data from network 125, converts it into a event data suitable for analysis by policy monitor 100, and forwards the event data to policy monitor 100. The event data is either collected and distributed or streamed in real time. Policy monitor 100 analyzes the received event data and transmits information about policy dispositions back to packet gathering component 128. This section of COOPER et al. does not disclose or even remotely suggest using at least one policy agent to inject packets at the at least one injection point, as required by claim 9. Rather, this section of COOPER et al. merely discloses transmitting event data to a policy monitor. Such disclosure does not relate to injection points in any manner whatsoever.

Page 14, paragraph [0289] of COOPER et al. discloses an agent descriptor "INTRANET_MONITOR." This section of COOPER et al. does not disclose determining at least one injection point based on the at least one policy point, as alleged by the Examiner. In fact, this section of COOPER et al. does not even relate to determining at least one injection point. As described in the present specification at paragraph [0130], "[i]njection points are determined based on the policy points defined in policy and service definitions, and on the flow of packets. For example, when there is one policy point and the flow is bi-directional, two injection points are needed. One injection point injects traffic from the subscriber to the content server and the other injection point injects traffic from the content server to the subscriber." Clearly, the cited

section of COOPER et al. does not relate to the injection points, as this term is recited in claim 9.

Page 14, paragraph [0292] of COOPER et al. discloses a wizard for segregating all intradomain ICMP traffic using a rule that assigns the traffic to the disposition "Monitor_Icmp." The rule is named by combining the protocol name (ICMP) with the domain name together with the word "_Within" to result in a rule named "Icmp_Within_Intranet." This section of COOPER et al. does not disclose or even remotely suggest determining at least one injection point based on the at least one policy point; using at least one policy agent to inject packets at the at least one injection point; or collecting statistics from some of the at least one policy agent, as required by claim 9. Rather, this section of COOPER et al. merely discloses a naming scheme whereby a rule name is generated based on a protocol and domain to which it applies.

Page 4, TABLE A of COOPER et al. discloses a listing of network security terminology relating to policy monitoring. TABLE A does not disclose or even remotely suggest collecting statistics from one of the at least one policy agent, as alleged by the Examiner. In fact, TABLE A does not even relate to a policy agent to inject packets at the at least one injection point.

For at least these additional reasons, claim 9 is not anticipated by COOPER et al. Reconsideration and allowance of claim 9 are therefore respectfully requested.

Independent claim 10, as amended, recites features similar to (yet possibly different in scope than) those set forth above with respect to claim 1. Accordingly, claim 10 is not anticipated by COOPER et al. for at least reasons similar to those set forth

above with respect to claim 1. Reconsideration and allowance of claim 10 are respectfully requested.

Claims 11, 12, 16, and 17 depend from claim 10 and are therefore not anticipated by COOPER et al. for at least the reasons set forth above with respect to claim 10. Moreover, these claims are not anticipated by COOPER et al. for reasons of their own.

For example, COOPER et al. does not disclose or suggest that the one or more devices are configured to command, via the agent interface, one or more agents to inject packets into a network, as required by claim 17. In rejecting claim 17, the Examiner indicated that page 6, paragraph [0108] of COOPER et al. allegedly disclose this feature (Office Action – pg. 6). Applicant respectfully disagrees.

At page 6, paragraph [0108], COOPER et al. discloses:

In another embodiment of the invention, the network monitor 127 can read packet data directly from observed network 125, generating a continuous stream of event updates for the policy monitor 100. This stream operates in real-time so that the policy monitor 100 processes events shortly after they happen on observed network 125.

This section of COOPER et al. discloses that collected packet data may be streamed from the observed network to policy monitor 100. This section of COOPER et al. does not disclose or suggest one or more devices that are configured to command, via the agent interface, one or more agents to inject packets into a network, as required by claim 17. In fact, this section of COOPER et al. does not even relate to injecting packets into a network, but rather merely relates to reading data from a network and generating event updates therefrom.

For at least this additional reason, claim 17 is not anticipated by COOPER et al. Reconsideration and allowance are respectfully requested.

Rejection Under 35 U.S.C. 103(a) based on COOPER et al. and HADDOCK et al.

Claims 3-6, 15, 18, and 22 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over COOPER et al. in view of HADDOCK et al. Applicant respectfully traverses this rejection.

A proper rejection under 35 U.S.C. § 103 requires that three basic criteria be met. First, there must be some suggestion or motivation, either in the references themselves, or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest *each and every claim feature*. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not the applicant's disclosure. *In re Vaack*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Applicant respectfully submits that the cited combination of COOPER et al. and HADDOCK et al. does not disclose or reasonably suggest the combination of features recited in claims 3-6, 15, 18, and 22.

Claims 3-6 depend from claim 1. The disclosure of HADDOCK et al. does not remedy the deficiencies in the disclosure of COOPER et al. noted above with respect to claim 1. Accordingly, claims 3-6 are allowable over the combination of COOPER et al. and HADDOCK et al. for at least the reasons set forth above with respect to claim 1.

Claims 15 and 18 depend from claim 10. The disclosure of HADDOCK et al. does not remedy the deficiencies in the disclosure of COOPER et al. noted above with respect to claim 10. Accordingly, claims 15 and 18 are allowable over the combination

of COOPER et al. and HADDOCK et al. for at least the reasons set forth above with respect to claim 10.

Claim 22 depends from claim 19. It should be noted that claim 19 presently stands rejected under 35 U.S.C. § 103(a) as being unpatentable over COOPER et al. in view of PIESCO. Accordingly, Applicant submits that a prima facie case of obviousness has not been made with respect to claim 22, given the absence of any alleged disclosure of PIESCO. For the purposes of the response, Applicant assumes that the rejection of claim 22 under COOPER et al. and HADDOCK et al. is erroneous and that the Examiner intended that claim 22 be rejected under the combination of COOPER et al., PIESCO, and HADDOCK et al. Clarification is respectfully requested.

Regardless of the preceding grounds of rejection, Applicant respectfully submits that the disclosure of HADDOCK et al. does not remedy the deficiencies in the disclosure of COOPER et al. noted below with respect to claim 19. Accordingly, claim 22 is allowable over either the combination of COOPER et al. and HADDOCK et al. or COOPER et al., PIESCO, and HADDOCK et al. for at least the reasons set forth below with respect to claim 19.

Rejection Under 35 U.S.C. 103(a) based on COOPER et al. and WESTERINEN et al.

Claims 7 and 8 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over COOPER et al. in view of WESTERINEN et al. Applicant respectfully traverses this rejection.

Claims 7 and 8 depend from claim 1. The disclosure of WESTERINEN et al. does not remedy the deficiencies in the disclosure of COOPER et al. noted above with respect to claim 1. Accordingly, claims 7 and 8 are allowable over the combination of

COOPER et al. and WESTERINEN et al. for at least the reasons set forth above with respect to claim 1.

Rejection Under 35 U.S.C. 103(a) based on COOPER et al. and PIESCO

Claims 19, 21, 23, and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over COOPER et al. in view of PIESCO. Applicant respectfully traverses this rejection.

Independent claim 19 recites a system for analyzing packet treatment in a network including a management server configured to load policy rules and service definitions to a router when a subscriber session is established; a database including definitions of policy rules, the service definitions, and a network configuration, the database being configured to be accessible by the management server; a policy analyzer configured to analyze packet treatment based on ones of the policy rules and the service definitions defined for a subscriber, the policy analyzer being configured to access the management server and the database; a policy analyzer agent configured to receive commands from the policy analyzer to inject packets into a network at an injection point; and a user input/output interface configured to provide input to the policy analyzer and receive analysis results from the policy analyzer. COOPER et al. and PIESCO do not disclose or suggest the features of claim 19.

For example, COOPER et al. and PIESCO do not disclose or suggest a policy analyzer agent configured to receive commands from the policy analyzer to inject packets into a network at an injection point. In rejecting claim 19, the Examiner admitted that COOPER et al. does not disclose this feature and relied on page 2, paragraph [0019] of

PIESCO for allegedly disclose this feature (Office Action – pg. 12). Applicant respectfully disagrees.

Page 9, paragraph [0019] of PIESCO discloses that a scenario building module 14 may provide a graphical user interface for receiving network configuration information, etc. The scenario building module also provides for scheduling analysis based on asset availability. The scenario building utility then generates configuration files for the network elements being analyzed. This section of PIESCO further discloses that the scenario building utility also controls traffic flow and injects traffic packets into a simulated network to allow for user control during execution of a scenario. This section of PIESCO does not disclose or suggest a policy analyzer agent configured to receive commands from the policy analyzer to inject packets into a network at an injection point, as required by claim 19. In fact, this section of PIESCO does not relate to injection points in any manner whatsoever. Additionally, this section of PIESCO does not disclose a policy analyzer agent configured to receive commands from the policy analyzer. Rather all operations in PIESCO are performed by the scenario building module.

For at least this reason, claim 19 is patentable over COOPER et al. and PIESCO. Reconsideration and withdrawal of the rejection of claim 19 are respectfully requested.

Claim 21 depends from claim 19 and is therefore patentable over the combination of COOPER et al. and PIESCO for at least the reasons set forth above with respect to claim 19. Reconsideration and withdrawal of the rejection of claim 21 are respectfully requested.

Independent claim 23 recites one or more network devices including an analyzer interface configured to receive commands from a policy analyzer and send information to

the policy analyzer; an injector for injecting traffic into a network upon receiving a command from the policy analyzer via the analyzer interface; and a statistics module configured to collect statistics of the injected traffic, the statistics module being further configured to send the collected statistics to a policy analyzer via the analyzer interface. COOPER et al. and PIESCO do not disclose or suggest the features of claim 23.

For example, COOPER et al. and PIESCO do not disclose or suggest an injector for injecting traffic into a network upon receiving a command from the policy analyzer via the analyzer interface. In rejecting claim 23, the Examiner admitted that COOPER et al. does not disclose this feature and relied on page 2, paragraph [0019] of PIESCO for allegedly disclosing this feature (Office Action – pg. 13). Applicant respectfully disagrees with the Examiner's interpretation of PIESCO.

As recited above, this section of PIESCO discloses that the scenario building utility controls traffic flow and injects traffic packets into a simulated network to allow for user control during execution of a scenario. This section of PIESCO does not disclose an injector for injecting traffic into a network upon receiving a command from the policy analyzer via the analyzer interface, as required by claim 23. Rather, this section of PIESCO merely discloses a user interface for defining network configurations.

For at least this reason, claim 23 is patentable over COOPER et al. in view of PIESCO. Reconsideration and allowance are respectfully requested.

Claim 24 depends from claim 23 and is therefore patentable over COOPER et al. and PIESCO for at least the reasons set forth above with respect to claim 23. Reconsideration and withdrawal of the rejection of claim 24 are respectfully requested.

Conclusion

As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references, assertions as to dependent claims, etc.) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such assertions/requirements in the future.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Robin C. Clark, Reg. No. 40956/
Robin C. Clark
Registration No. 40,956

Date: September 17, 2007

11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
(571) 432-0800

Customer Number: 44987